(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 282 260 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.02.2003 Bulletin 2003/06

(51) Int Cl.7: **H04L 9/08**

(21) Application number: **02016814.2**

(22) Date of filing: **26.07.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.07.2001 DE 10137152**

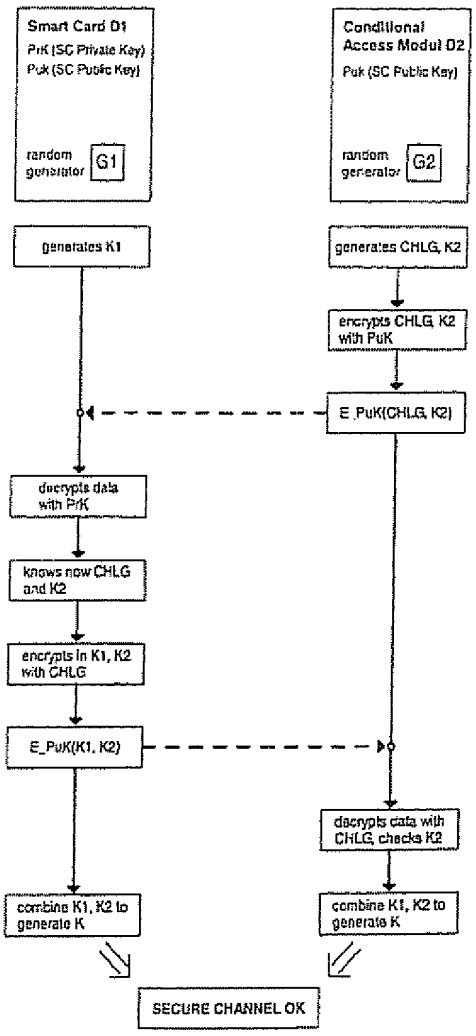
(71) Applicant: **SCM Microsystems GmbH**
85737 Ismaning (DE)

(72) Inventor: **Loisel, Yann**
13600 La Ciotat (FR)

(74) Representative: **Degwert, Hartmut, Dipl.-Phys.**
Prinz & Partner GbR,
Manzingerweg 7
81241 München (DE)

(54) Key agreement method for secure communication system

(57) For transmitting confidential data, two devices (D1, D2) are linked through a transmission channel which is secured by symmetric encryption with a shared secret session key. Both devices (D1, D2) possess the same secret session key (K) which is developed from two random keys (K1, K2) each of which is generated in a different one of the devices. Both random keys are exchanged between the devices (D1, D2) using asymmetric encryption.



EP 1 282 260 A1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a method of transmitting confidential data between two communication devices and, in particular, to a method of secure communication between a chipcard and a conditional access module (CAM) in a pay TV environment.

[0002] EP 0 720 326 A2 discloses a method of establishing a secure communication channel between two similar stations. The communication procedure uses symmetric encryption/decryption one to avoid problems encountered with earlier systems where a distributed master key is used in conjunction with modifier elements such as a time stamp, a counter or the like. In the symmetric procedure, a secret encryption key is known to both communication devices. This method only works with paired communication devices.

[0003] In another method that is disclosed in WO 97/38530, a secure communication between two devices such as a CAM and a chipcard is obtained by asymmetric encryption. One of the devices generates a random key which is encrypted with a public key and sent to the second device. The second device decrypts the encrypted key with a corresponding private key. Both devices use the random key for encryption and decryption of data exchanged between the devices. This method relies on a random value generated in only one of the devices.

[0004] The present invention provides a secure method of transmitting data between two communication devices which relies on a common secret based on two values each of which is generated by a different one of the devices, thereby avoiding possible replay attacks. According to the invention, the method of transmitting data between two communication devices includes the following steps:

Step 1: a first random key is generated on the side of the first communication device.

Step 2: a second random key is generated on the side of the second communication device.

Step 3: the second random key is encrypted by means of a public key and transmitted to the first communication device.

Step 4: on the side of the first communication device, the transmitted second random key is decrypted with a corresponding private key.

Step 5: the first random key is encrypted on the side of the first communication device and transmitted to the second communication device.

Step 6: the second communication device decrypts the transmitted first random key.

Step 7: each communication device combines the random keys into a secret session key used for encryption and decryption of the data transmitted between the devices.

[0005] After step 7, both devices share a secret session key based on two random values generated independently of each other and in different devices, thereby excluding the possibility of a successful replay attack.

[0006] A further improvement of the method is achieved by using a particular encryption key for encryption of the first random key in steps 5 and 6: in addition to the second random key, a random number (a "challenge") is generated on the side of the second communication device, and this random number is likewise encrypted with the public key and transferred to the first communication device. The first communication device decrypts the random number with its private key, and the first random key is encrypted with the decrypted random number prior to the transmission of the first random key to the second communication device.

[0007] A preferred embodiment of the invention will now be disclosed with reference to the drawing. The single figure of the drawing illustrates essential steps of the preferred embodiment.

[0008] With reference to the drawing, a first communication device D1 is a Smart Card (SC) and a second communication device D2 is a conditional access module (CAM) in a digital pay TV environment (DVB, for example), although the invention is not limited to application in such an environment. Both devices D1 and D2 would exchange confidential data, such as entitlement management messages (EMMs), entitlement control messages (ECMs) and control words (CWs). To protect the confidential data from eavesdropping, a secure communication channel is established between the devices D1, D2.

[0009] The first device D1 owns a secret private key PrK and has a corresponding public key PuK. Device D1 also has a random number generator G1.

[0010] The second device D2 knows the public key PuK, which may have been received from device D1 in the clear. Device D2 also has a random number generator, G2.

[0011] Initially, both devices D1, D2 do not share any secret. In order to provide a secret session key shared by the devices and used for encryption/decryption of data exchanged between the devices, a protocol is proposed that is safe enough to avoid leakage of information, and powerful enough to exchange keys of a sufficient length. The protocol involves asymmetric cryptography for transmission both from D1 to D2 and from D2 to D1.

[0012] Random number generator G1 in device D1 internally generates a first random number K1. Random number generator G2 in device D2 internally generates a second random number K2. D2 will also generate a further random value, a "challenge" CHLG. Random

numbers K1 and K2 are of a sufficient length to avoid crypto-analytic brute-force attack.

[0013] Device D2 encrypts K2 and CHLG with public key PuK and sends the result to device D1. Device D1 will receive the result and decrypt it with its private key PrK. Device D1 now knows K2 and CHLG. Device D1 concatenates K2 with its own random number K1 and encrypts the concatenated numbers with CHLG. The encrypted result is sent from D1 to D2.

[0014] Device D2 now decrypts the received result to K1 and K2 using CHLG as the decryption key to retrieve K1 and K2. D2 checks for consistency of received K2 with its own K2. If the correct K2 has been received, both devices D1 and D2 now share both random numbers K1 and K2.

[0015] Finally, both devices D1 and D2 will combine random keys K1 and K2 in the same manner to provide a secret session key K now owned by both devices. Session key K is used for symmetric encryption and decryption of confidential data exchanged between the devices.

[0016] Another example for use of the invention is a conditional access module (CAM) as the first device D1 and a decoder in a Set-Top-Box (STB) as the second device D2. Here, too, confidential data would be exchanged using a session key for encryption/decryption that originates from two random numbers each generated in a different one of the devices.

Claims

1. A method of transmitting confidential data between two communication devices, in which

   a) a first random key (K1) is generated on the side of the first communication device (D1);
   b) a second random key (K2) is generated on the side of the second communication device (D2);
   c) the second random key (K2) is encrypted by means of a public key (PuK) and transmitted from the second (D2) to the first (D1) communication device;
   d) on the side of the first communication device (D1), the transmitted second random key (K2) is decrypted using a corresponding private key (PrK);
   e) the first random key (K1) is encrypted on the side of the first communication device (D1) and transmitted to the second communication device (D2);
   f) the first communication device (D1) decrypts the transmitted first random key (K1); and
   g) both communication devices (1, 2) combine the random keys (K1, K2) to a secret session key (K) used by each device (D1, D2) for symmetric encryption and decryption of the confidential data.

2. The method according to claim 1, in which

   h) in addition to the second random key (K2), a random number (CHLG) is generated on the side of the second communication device (D2);
   i) the random number (CHLG) is likewise encrypted by means of the public key (PuK) and transferred to the first communication device (D1);
   j) the random number (CHLG) is decrypted by the first communication device (D1) using its private key (PrK);
   k) the first random key (K1) is encrypted with the random number (CHLG) prior to being transmitted to the second communication device (D2).

3. The method according to claim 2, in which

   l) the first communication device (D1) encrypts the second random key (K2) and transmits it to the second communication device (D2);
   m) the second communication device (D2) decrypts the transmitted second random key (K2) and checks its integrity by comparison with the original second random number (K2).

4. The method according to claim 2, in which

   n) the first communication device (D1) decrypts the second random key (K2) using the random number (CHLG) and transmits it to the second communication device (D2);
   o) the second communication device (D2) decrypts the transmitted second random key (K2) using the random number (CHLG) and checks its integrity by comparison with the original second random key (K2).

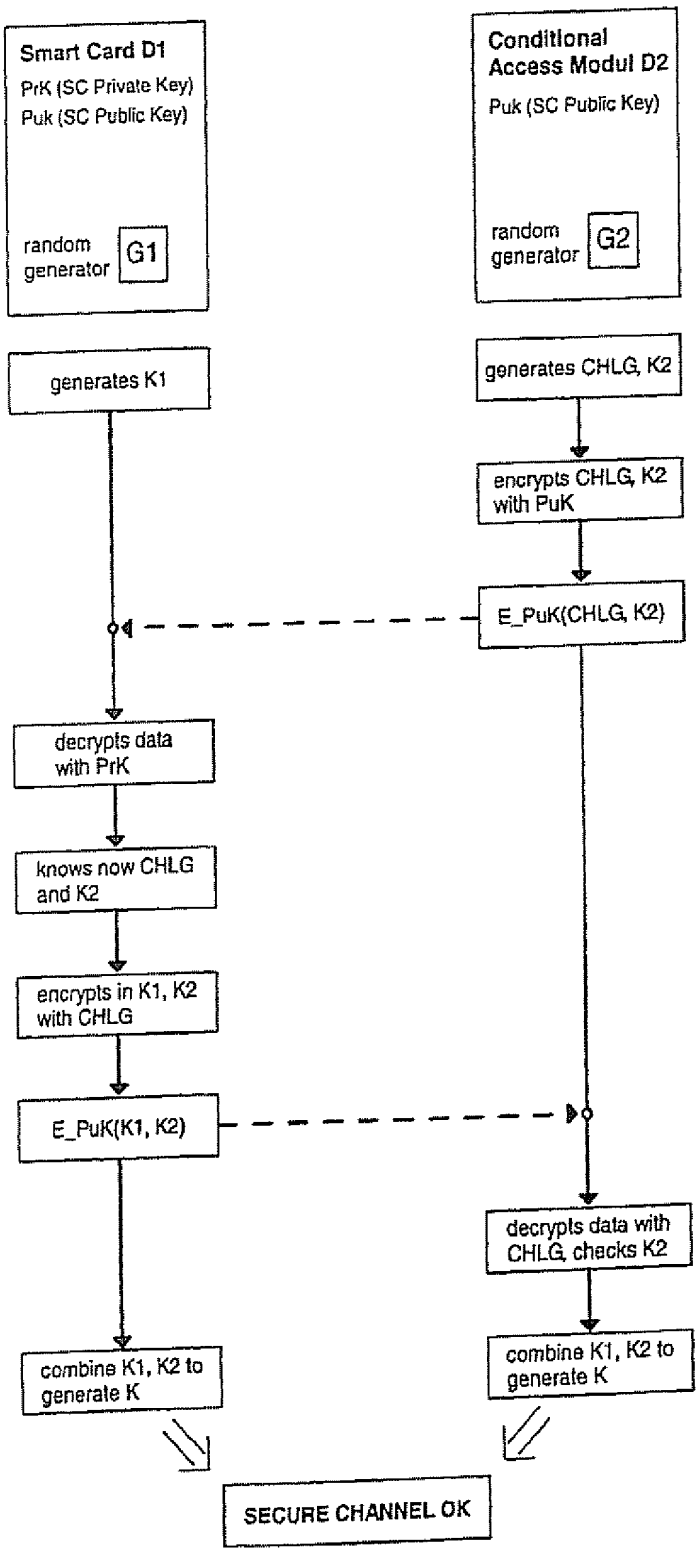
5. The method according to any of the preceding claims, in which the session key (K) is developed so as to have the same length as each of the first and second random keys (K1, K2).

6. The method according to any of the preceding claims, in which the first and second random keys (K1, K2) are each produced by a respective random number generator G1, G2) of the first and second communication device (D1, D2).

7. The method according to any of the preceding claims, in which the first communication device (D1) is a smart card and the second communication device (D2) is a conditional access module (CAM).

8. The method according to any of claims 1 to 6, in

which the first communication device (D1) is a conditional access module (CAM) and the second communication device (D2) is a decoder in a Set-Top-Box (STB).


Smart Card D1
PrK (SC Private Key)
Puk (SC Public Key)
random generator
G1
Conditional Access Modul D2
Puk (SC Public Key)
random generator
G2
generates K1
generates CHLG, K2
encrypts CHLG, K2 with PuK
E_PuK(CHLG, K2)
decrypts data with PrK
knows now CHLG and K2
encrypts in K1, K2 with CHLG
E_PuK(K1, K2)
decrypts data with CHLG, checks K2
combine K1, K2 to generate K
combine K1, K2 to generate K
SECURE CHANNEL OK

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 01 6814

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	EP 0 537 971 A (MOTOROLA INC) 21 April 1993 (1993-04-21) * column 3, line 10 - line 27 * * column 4, line 36 - column 7, line 45 * * column 10, line 49 - column 11, line 6 * * figure 5 * ---	1-8	H04L9/08
X	US 5 371 794 A (AZIZ ASHAR ET AL) 6 December 1994 (1994-12-06) * column 1, line 42 - column 2, line 19 * * column 8, line 43 - column 9, line 12 * * column 10, line 25 - line 65 * ---	1-8	
X	EP 0 739 106 A (CERTICOM CORP) 23 October 1996 (1996-10-23) * column 5, line 25 - column 7, line 15 * ---	1-8	
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 13, 30 November 1999 (1999-11-30) & JP 11 234259 A (HITACHI LTD), 27 August 1999 (1999-08-27) * abstract * -----	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 October 2002	Bec, T

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 01 6814

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-10-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0537971 A	21-04-1993	US 5179591 A	12-01-1993
		AU 655304 B2	15-12-1994
		AU 2202092 A	29-04-1993
		DE 69217440 D1	27-03-1997
		DE 69217440 T2	07-08-1997
		DK 537971 T3	07-07-1997
		EP 0537971 A2	21-04-1993
		HK 1007367 A1	09-04-1999
		IE 922612 A1	21-04-1993
		JP 5227152 A	03-09-1993
		KR 234447 B1	15-12-1999
		NO 923371 A	19-04-1993
		US 5341427 A	23-08-1994
		US 5230020 A	20-07-1993
US 5371794 A	06-12-1994	EP 0651533 A2	03-05-1995
		JP 7193569 A	28-07-1995
		US RE36946 E	07-11-2000
EP 0739106 A	23-10-1996	US 2001042205 A1	15-11-2001
		AU 5266696 A	07-11-1996
		CA 2174260 A1	22-10-1996
		WO 9633566 A1	24-10-1996
		EP 0739106 A1	23-10-1996
JP 11234259 A	27-08-1999	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82